Product Support Notice

PSN #	PSN005435u				
Original publication date: June 25, 2019 This is Issue #01, published date: June 25, 2019.		Severity/risk level	High	Urgency	Immediately

Name of problem

New Certificate Requirements for Android Q and iOS 13 Operating Systems

Products affected

IP Office
Powered by Avaya IP Office (Virtualized)
Powered by Avaya IP Office (Containerized)
Avaya Equinox® (Android, iOS)
Client SDK (Android, iOS)
Avaya one-X Mobile (Android, iOS)
Avaya Communicator for iPad
Avaya Communicator for Web (Chrome on macOS)
Video Softphone for Mac
Safari browser (access to IP Office web applications e.g. Web Manager)

Problem description

This PSN advises customers and partners of changes in the Android Q, iOS 13 and macOS 10.15 operating systems that may impact operation of the noted IP Office clients. If the IP Office server certificates in use do not meet the new requirements, those IP Office clients **running on the new OS versions** will not be able to connect, and services will be unavailable to users on those new OS versions.

Android Q

As of Android Q, which is currently in Beta, Google is dropping support for SHA1 and SHA-2 CBC signature algorithms. If any servers used by the IP Office clients have identity certificates signed using these signature algorithms, the client will not be able to connect to those servers.

iOS 13 and macOS 10.15.

On June 3rd, Apple announced new requirements for trusted certificates in iOS 13 and macOS 10.15 both of which are currently in beta:

- TLS server certificates and issuing CAs using RSA keys must use key sizes greater than or equal to 2048 bits. Certificates using RSA key sizes smaller than 2048 bits are no longer trusted for TLS.
- TLS server certificates and issuing CAs must use a hash algorithm from the SHA-2 family in the signature algorithm. SHA-1 signed certificates are no longer trusted for TLS.
- TLS server certificates must present the DNS name of the server in the Subject Alternative Name extension of the certificate. DNS names in the CommonName of a certificate are no longer trusted.

Additionally, all TLS server certificates issued after July 1, 2019 (as indicated in the NotBefore field of the certificate) must follow these guidelines:

- TLS server certificates must contain an ExtendedKeyUsage (EKU) extension containing the id-kp-serverAuth OID.
- TLS server certificates must have a validity period of 825 days or fewer (as expressed in the NotBefore and NotAfter fields of the certificate).

Connections to TLS servers violating these new requirements will fail and may cause network failures, apps to fail, and websites to not load in Safari in iOS 13 and macOS 10.15.

See https://support.apple.com/en-us/HT210176 for complete details.

Background

Please refer to IP Office Security Guidelines (https://downloads.avaya.com/css/P8/documents/101047519) for more information on managing and upgrading security certificates for IP Office environments.

The default self-signed IP Office identity certificate meets the new requirements above except for validity period and inclusion of ExtendedKeyUsage (EKU) extension. Default validity period is seven (7) years and any regenerated IP Office server identity certificates do not include EKU.

Note that the default / internally generated IP Office server identity certificates will only be an issue (1) for identity certificates generated after July 1st, 2019 and (2) in case of client connections from iOS 13 / macOS 10.15.

Any IP Office systems using a default self-signed identity certificate already generated prior to July 1st, 2019 will not experience an issue with those certificates; and any clients running on OS prior to iOS 13 / macOS 10.15 will not have an issue with default self-signed identity certificates generated after July 1st, 2019.

Resolution

To ensure ongoing operation of the IP Office clients noted, you must assess the certificates installed on all servers used in your environment by those clients and update any certificates to meet the requirements for all Android, iOS and macOS devices in use.

Do not use / regenerate any default self-signed IP Office server identity certificates from 1st July 2019, if client connections will be required from iOS 13 / macOS 10.15. This PSN will be updated once additional resolutions are available.

Any third-party identity certificates should be checked to ensure as soon as possible that they do comply with the new requirements.

Workaround or alternative remediation

Avoid installing any beta version of Android Q, iOS 13 and macOS 10.15 until updated certificates have been deployed, if use of the IP Office clients noted is required. This PSN will be updated once additional resolutions are available.

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions

Service-interrupting?

n/a

No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.